UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff, Case No. 19-CR-02

vs.

ALEXANDER P. BEBRIS,

Defendant.

DEFENDANT'S BRIEF IN SUPPORT OF HIS MOTION TO SUPPRESS EVIDENCE AND STATEMENTS

Alexander P. Bebris, by and through his attorneys Gimbel, Reilly, Guerin & Brown LLP, submits the following brief in support of his motion to suppress evidence and statements, pursuant to the Fourth, Fifth and Sixth Amendments of the United States Constitution, *Katz v. U.S.*, 389 U.S. 347, 88 S.Ct. 507 (1967), and *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 109 S.Ct. 1402 (1989).

Bebris believes the evidence will show that through its agents, the government conducted illegal searches which resulted in the discovery of allegedly incriminating evidence against Bebris, and this Court should suppress the resulting physical evidence and statements. Alternatively, should this Court determine no government agent conducted an initial search, the government impermissibly expanded the initial private search.

FACTS

According to the pleadings and police reports associated with this case, on December 13, 2018, The Internet Crimes Against Children Task Force ("ICAC") contacted the Winnebago County Sheriff's Office regarding CyberTips ICAC received from the National Center for Missing and Exploited Children ("NCMEC"), which initially received the CyberTips from Facebook.

There are two CyberTips at issue here: (1) CyberTip 39932621, which occurred on September 6, 2018, at 13:25:46 UTC and included two images of suspected child pornography associated with Facebook username "Alexander Bebris"; and (2) CyberTip 40017882, which occurred on September 9, 2018, at 17:04:49 UTC and included one image of suspected child pornography associated with Facebook username "Alexander Paul." According to the CyberTips, Facebook username "Carly Macks" was the intended recipient of these images. Both Detective Hammen and Investigator Sewall of the Winnebago County Sheriff's Office reviewed the images included in the CyberTips; and the CyberTips resulted in administrative subpoenas issued on December 7, 2018, for each of the Facebook accounts.

On December 17, 2018, Detective Hammen completed a search warrant application and affidavit based on the CyberTips for Bebris's address. In his affidavit, Detective Hammen stated:

> Your affiant is informed, from his personal observations, and the reports of the National Center for Missing and Exploited Children and the Wisconsin Department of Justice – Division of Criminal Investigations, which have proven to be reliable in the past, that on 12/13/18 at 08:37 hours Megan Paskey of the Wisconsin ICAC Taskforce Division of Criminal Investigation contacted the Winnebago County Sheriff's Office requesting to investigate two related

> CyberTips. DCI Paskey referred CyberTip 39932621 and 40017882 to Investigator Michael Sewall W203 of the Winnebago County Sheriff's Office and your affiant. Investigator Sewall and your affiant received the CyberTip information from the ICAC Data System. The IDS system also sent an email notification regarding these CyberTips.

The affidavit went on to detail the two individual CyberTips, the contents of the CyberTips, and the fact that Investigator Sewall and Detective Hammen viewed each of the images contained in the CyberTips.[1] The search warrant was subsequently signed, and on December 19, 2018, the government conducted a search of Bebris's home. During the search, Detective Hammen spoke to Bebris. Bebris indicated he was the only person living in his residence, that he had lived there since February 2018, and that he had secured Spectrum WiFi.

The government's search resulted in multiple items seized including four mobile phones, five thumb drives, one CD, one SD card, three hard drives, a Dell Laptop, a Dell computer, Bebris's passport, and a document containing Bebris's name and address. Additionally, Investigator Sewall viewed a piece of paper containing a file string which included the term "TOR." During the search, the government examined the Dell computer located in Bebris's residence on-site. This examination resulted in eighty-nine "files of interest" and the government arrested Bebris for ten counts of possession of child pornography. Bebris was subsequently indicted on one count of distribution of child pornography and one count of possession of child pornography.

[1] The CyberTips referenced in the search warrant affidavit are not in the discovery and have not been provided.

Hash Values

Hash values are akin to a fingerprint of a photo. Hash values are "numeric value[s] of a fixed length that uniquely identifies data. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures." Meyer Aff. at ¶2, Ex. A (quoting Microsoft.NET, *Ensuring Data Integrity with Hash Codes*, Mar. 29, 2017 (available at https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes)). Essentially, when two images have the same hash value, "then it is forensically sound to conclude that both values indicate the same [material]." *Id.*

NCMEC

According to its website, NCMEC is "the nation's clearinghouse and comprehensive reporting center for all issues related to the prevention of and recovery from child victimization. See National Center for Missing & Exploited Children, http://www.missingkids.com/home (last visited August 20, 2019). [2] The agency boasts reporting 424,066 missing children to law enforcement in the United States in 2018. *Id.* NCMEC was founded in 1984 and by 1998 NCMEC had created their CyberTipline – "a centralized reporting mechanism for the public and electronic service providers to report suspected child sexual exploitation." Dep't of Justice, *National Strategy for Child*

[2] The articles and materials referenced herein are attached to the affidavit of Brianna J. Meyer.

Exploitation Prevention and Interdiction, Report to Congress (April 2016), retrieved from https://www.justice.gov/psc/file/842411/download.

In 2006, NCMEC collaborated with leaders of the Technology Coalition (comprised of various Internet leaders) to combat online material containing child sexual abuse. Thorn Staff, *Eliminating Child Sexual Abuse Material: The Role and Impact of Hash Values*, THORN, (published April 18, 2016), https://www.thorn.org/blog/eliminating-child-sexual-abuse-material-hash-values/. The basic premise of the collaboration was that NCMEC would provide electronic service providers ("ESPs") with hash values of child pornography previously reported to NCMEC's CyberTipline in order to further detect any potentially illegal conduct. *Id.*

PhotoDNA and PhotoDNA Signatures

In 2009, Microsoft developed a program called PhotoDNA and donated the program to NCMEC. Dan Sytman, *Facebook And Microsoft Team Up To Tackle Child Pornography*, Washington State Office of the Attorney General, (posted on March 20, 2011), https://www.atg.wa.gov/in-general-blog/facebook-and-microsoft-team-tackle-child-pornography (internal citations omitted). PhotoDNA creates hash values of images that allow ESP's to more readily detect child pornography. Meyer Aff. at ¶2 Ex. A. Since its development, PhotoDNA has been credited as "one of the most significant tools ever created in the reduction of child sexual abuse material online." Staff, *Eliminating Child Sexual Abuse Material*.

Not only did Microsoft donate PhotoDNA to NCMEC, it also "granted NCMEC the legal right to sublicense this technology for free to domestic and foreign ESPs

interested in taking proactive steps to identify and eliminate child pornography from their servers." Dep't of Justice, *National Strategy for Child Exploitation Prevention and Interdiction*.

PhotoDNA also has a database of known hash values, called PhotoDNA signatures. "These NCMEC-generated PhotoDNA signatures and hash values are derived from ***apparent*** child pornography images that have been reported by U.S.-based ESPs to NCMEC's CyberTipline." Dep't of Justice, *National Strategy for Child Exploitation Prevention and Interdiction* (emphasis added). Once an ESP licenses PhotoDNA from NCMEC, NCMEC can also allow the ESP access to its set of PhotoDNA signatures. Dep't of Justice, *National Strategy for Child Exploitation Prevention and Interdiction*.

Facebook's Cooperation with NCMEC

Facebook first began using PhotoDNA technology with NCMEC and Microsoft in early 2011. Sytman, *Facebook And Microsoft Team Up To Tackle Child Pornography*. Facebook has explained its relationship with NCMEC in the following manner:

> We have specially trained teams with backgrounds in law enforcement, online safety, analytics, and forensic investigations, which review content and report findings to NCMEC. In turn, NCMEC works with law enforcement agencies around the world to help victims, and we're helping the organization develop new software to help prioritize the reports it shares with law enforcement in order to address the most serious cases first.

Andrew Hutchinson, *Facebook Outlines Enhanced Efforts to Remove Child Exploitation Content from its Platform*, Social Media Today, (published October 25, 2018), https://www.socialmediatoday.com/news/facebook-outlines-enhanced-efforts-to-remove-child-exploitation-content-fro/540505/ (quoting posts from Facebook); see also Antigone Davis, Global Head of Safety at Facebook, *New Technology to Fight Child*

Exploitation, Facebook Newsroom, (published October 24, 2018), https://newsroom.fb.com/news/2018/10/fighting-child-exploitation/.

The relationship is more intricate and coordinated than it appears. Facebook and NCMEC's partnership dates back years, and Facebook has long used the PhotoDNA software provided by NCMEC. NCMEC, *Corporate Partners: Facebook*, (last visited May 28, 2019), http://api.missingkids.org/partners/Facebook.; Larry Magid and Michelle DeLaune, *NCMEC's COO Michelle DeLaune on how Facebook combats so-called 'child porn,'* Blog Talk Radio, (published Oct. 2018), http://www.blogtalkradio.com/connectsafely/2018/10/24/ncmecs-coo-michelle-delaune-on-how-facebook-combats-so-called-child-porn.

According to Chris Sonderby, assistant general counsel at Facebook, the company runs the PhotoDNA software on ***all*** images uploaded to its platform and the software aids Facebook in notifying both NCMEC and the police for immediate action. Microsoft Digital Crimes Unit, *PhotoDNA; The Next Chapter in Protecting Children Online*, YouTube (May 19, 2011), https://www.youtube.com/watch?v=7pFMV8rl_2Y. Additionally, Facebook provides both financial and technical support to NCMEC, and allows NCMEC to use its "networking capabilities [which is] a very powerful tool used by [NCMEC] to distribute photos of missing children, eradicate child exploitation images, and share information for parents and teens about how to be safe in both the online and real world." NCMEC, *Corporate Partners: Facebook*.

The relationship between NCMEC and Facebook appears to only be growing stronger and closer over time. In recent years, Facebook and NCMEC teamed up to

launch a new Amber Alert program to give Facebook users information of how they can help missing children. Wall Street Hedge, *Facebook Teams Up With NCMEC To Find Mising Children Via Amber Alerts*, (last visited May 28, 2019), https://www.wallstreethedge.com/facebook-teams-up-with-ncmec-to-find-missing-children-via-amber-alerts/21494/. Furthermore, as the number of reports of child pornography is on the rise, NCMEC said it is working with Facebook to develop software to decide which tips to assess first." Dave Paresh, *Facebook removed 8.7 million images of child nudity with a new machine learning software,* Business Insider, (published Oct. 24, 2018), https://www.businessinsider.com/r-facebook-unveils-systems-for-catching-child-nudity-grooming-of-children-2018-10.

Not only does Facebook work directly with NCMEC, but Facebook also works with various law enforcement agencies, including the Los Angeles ICAC unit and the Texas Attorney General's office. Larry Magid, *How Facebook Fights Child Porn*, (published May 8, 2012), https://www.cnet.com/news/how-facebook-fights-child-porn/ (internal quotations omitted). Law enforcement agencies credit Facebook for their constant communication and involvement in trying to combat criminal activity. *Id.* Additionally, Former Washington State Attorney General Rob McKenna left a recorded message for employees of Facebook and Microsoft after the launch of PhotoDNA expressing gratitude for the creation of PhotoDNA and Facebook's deployment of the program. Sytman, *Facebook And Microsoft Team Up To Tackle Child Pornography*.

ARGUMENT

The Fourth Amendment protects "against unreasonable searches and seizures." U.S. CONST. AMEND. IV. Individuals have a right to be free from such unreasonable conduct by the government and its agents. *Id.* However, this Circuit has not yet decided whether certain technologies and corporations (namely, NCMEC, PhotoDNA, and Facebook) can act as a government agent.

NCMEC consistently acts as a government agent when it sublicenses the PhotoDNA software to ESP's and evaluates CyberTips. Furthermore, PhotoDNA and Facebook each act as NCMEC's agent and therefore as an agent of the government. Additionally, Bebris had a subjective expectation of privacy in his Facebook messages that was objectively reasonable. Therefore, this Court should suppress all evidence and statements derived from the illegal initial search and subsequent searches.

In the alternative, should this Court find that neither NCMEC nor PhotoDNA nor Facebook acts as a government agent, law enforcement impermissibly expanded the scope of the initial private search in its subsequent searches and this Court should suppress the physical evidence and testimony derived from the search. Bebris respectfully requests an evidentiary hearing on the matter, leave to file any necessary additional briefing after the hearing, and for this Court to subpoena certain individuals to testify at the hearing.

I. NCMEC, PhotoDNA, and Facebook Each Acted as an Agent of the Government.

> [F]or what would have been the point of the [Fourth Amendment] if the government could have instantly rendered it a dead letter by the simple expedient

> of delegating to agents investigative work it was forbidden from undertaking itself?

United States v. Ackerman, 831 F.3d 1292, 1300 (10th Cir. 2016).

It has long been held that a court may find a private party acted as a government agent, and therefore was subject to the Fourth Amendment provisions. "Agency is the fiduciary relation which results from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act." Restatement (Second) of Agency §1. The government cannot "evade the most solemn obligations imposed in the Constitution by simply resorting to corporate form." *Lebron v. National R.R. Passenger Corp.*, 513 U.S. 374, 397, 115 S.Ct. 961 (1995).

A court's analysis of whether a private party acts as a government agent "must be made on a case-by-case basis and in light of all the circumstances" and is guided by common agency law. *United States v. Koenig*, 568 F.2d 843, 847 (7th Cir. 1988) (internal quotations omitted); see also *Skinner*, 489 U.S. at 615-16, 109 S.Ct. 1402 (the Court asked whether "the Government's encouragement, endorsement, and participation" in testing was enough to render private railroads government agents under the Fourth Amendment). The common law traditionally does not require "that the agent be an altruist, acting without any intent of advancing some personal interest along the way (like monetary gain) . . . Instead the question is usually simply whether the agent acts with the principal's consent and (in some way) to further the principal's purpose." *Ackerman*, 831 F.3d at 1301 (citing Restatement (Second) of Agency §§387-93)).

The Seventh Circuit employs a two-part test to determine whether a private party acts as a government agent: (1) "whether the government knew of and acquiesced in the intrusive conduct;" and (2) "whether the private party's purpose . . . was to assist law enforcement efforts or to further his own ends." *United States v. McAllister*, 18 F.2d 1412, 1417 (7th Cir. 1994) (quoting *United States v. Feffer*, 831 F.2d 734, 739 (7th Cir. 1987)).

NCMEC Acted as a Government Agent

"[E]ven an admittedly private entity can be made into a public one later by sufficient statutory action." *United States v. Ackerman*, 831 F.3d 1292, 1299 (10th Cir. 2016). As the Tenth Circuit held in *Ackerman*, the statutory action surrounding NCMEC in conjunction with the facts of this case has rendered it a government agent. *Id.*

While the exact conduct of NCMEC in this case is unclear, what ***is*** clear is NCMEC's level of cooperation with the government. Congress has imposed statutes that give NCMEC powers and responsibilities equivalent with Government agencies. See, *e.g.*, 42 U.S.C. §5773(b). NCMEC alone is responsible for its CyberTipline, NCMEC alone is the body ESP's must report any known child pornography to, and NCMEC alone may knowingly receive child pornography and intentionally view it without criminal penalty. *Ackerman*, 831 F.3d at 1296-97; 18 U.S.C. §2258A(a)-(c), (e). Additionally, 34 U.S.C. §11293(b) expressly delineates numerous functions NCMEC ***shall*** perform. These functions are explicitly considered "duties and responsibilities under Federal law to assist or support law enforcement agencies in the administration of criminal justice functions." 34 U.S.C. §20961.

Moreover, once NCMEC confirms a CyberTip, the reporting ESP must treat that confirmation as a request to preserve evidence issued by the government. *Ackerman*, 831 F.3d at 1297. Courts can impose civil or criminal sanctions against ESPs that do not comply with the NCMEC rules. *Id.* at 1296. Thus, the government constantly knows of and acquiesces to NCMEC's intrusive conduct.

Furthermore, NCMEC's purpose in general is to assist law enforcement. NCMEC makes no secret of how much its efforts have aided law enforcement in locating and prosecuting child pornography. For example, its website's front page contains a large banner stating how many children were reported to law enforcement through CyberTips in 2018. National Center for Missing & Exploited Children, http://www.missingkids.com/home. NCMEC is also statutorily obligated to assist in criminal prosecutions. See 18 U.S.C. §2258A(c). Here, the police reports show that NCMEC provided two CyberTips to law enforcement for the prosecution of alleged possession of child pornography.

This Court should conclude as then Judge, now Justice, Neil Gorsuch did in the *Ackerman* case that NCMEC should be treated, for Fourth Amendment purposes, as a government agent. The government's knowledge and acquiescence of NCMEC's invasive conduct as well as NCMEC's purpose of assisting law enforcement, supports the conclusion that NCMEC acted, and continues to act, as a government agent. Therefore, the Fourth Amendment applies to its conduct.

PhotoDNA Acted as a Government Agent

In addition to NCMEC, PhotoDNA also acts as a government agent. The United States Supreme Court has held that technology that enhances investigate abilities of law enforcement can trigger the Fourth Amendment protections. See *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 2043 (2001) ("To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use." (internal quotations omitted)).

PhotoDNA is a program created for NCMEC by Microsoft, donated to NCMEC, and a program which NCMEC has the right to sublicense. Sytman, *Facebook And Microsoft Team Up To Tackle Child Pornography*. In addition, NCMEC maintains a database with hash values of apparent child pornography which PhotoDNA uses to search various content. Dep't of Justice, *National Strategy for Child Exploitation Prevention and Interdiction*. NCMEC, as a government agent, employs PhotoDNA to continuously scan all photos uploaded or shared on websites of ESP's that partner with NCMEC to determine if any child pornography exists on the ESPs' webpages. *Id.*

PhotoDNA rises to the level of a government agent. First, NCMEC knows of and acquiesces to the intrusion by PhotoDNA. NCMEC has been licensing and sublicensing PhotoDNA since its inception approximately ten years ago. Sytman, *Facebook And*

Microsoft Team Up To Tackle Child Pornography. There was no question to NCMEC at the time of Bebris's alleged messages, and there is no question to NCMEC now, as to how PhotoDNA operated or how it would invade individuals' social media profiles. NCMEC has employed PhotoDNA for approximately eight years and shows no sign of stopping any time soon. In fact, NCMEC credits PhotoDNA for the uptick in child pornography CyberTips. Staff, *Eliminating Child Sexual Abuse Material: The Role and Impact of Hash Values*.

Further, PhotoDNA's entire purpose is to aid the government in investigating and prosecuting crimes. The software is licensed exclusively to a government policing agency – NCMEC – and is distributed by NCMEC to various ESPs. Sytman, *Supra;* Dep't of Justice, *National Strategy for Child Exploitation Prevention and Interdiction*. Thus, PhotoDNA is a government agent and its conduct is limited by the Fourth Amendment.

Facebook Acted as a Government Agent

Finally, Facebook is also an agent of NCMEC and therefore an agent of the government. Not only is Facebook statutorily compelled to cooperate with NCMEC, Facebook and NCMEC have an intricate, coordinated, and consistently growing relationship to investigate crimes.

To begin, 18 U.S.C. §2258A demands that any ESP shall, after obtaining knowledge of child pornography, "provid[e] to the CyberTipline of NCMEC, or any successor to the CyberTipline operated by NCMEC, the mailing address, telephone number, facsimile number, electronic mailing address of, and individual point of contact for, such provider"

and "mak[e] a report of such facts or circumstances to the CyberTipline . . ." However, Facebook and NCMEC's relationship goes far beyond statutes.

Facebook dedicates "specially trained teams" to work with NCMEC and help it develop new software for reporting child pornography. Hutchinson, *Facebook Outlines Enhanced Efforts to Remove Child Exploitation Content from its Platform*. The two agencies have had this relationship for years and Facebook provides technological and financial support to NCMEC. NCMEC, *Corporate Partners: Facebook*.

Although Facebook does have private interests in keeping child pornography off its website, a party "may be the servant of two masters, not joint employers, at one time as to once act, provided that the service to one does not involve abandonment of the service to the other." Restatement (First) of Agency §226. Here, Facebook and NCMEC have the same goal when it comes to child pornography on Facebook – to completely eradicate it. Facebook's desire to help NCMEC in no way abandons service to its private interests.

NCMEC, and therefore the government, is aware of Facebook's consistent searches of user profiles and Facebook acts with a purpose of helping the government. So, Facebook is an agent of the government and its continuous searches of user data falls within the bounds of the Fourth Amendment.

II. Bebris Believes the Evidence Will Show that NCMEC, PhotoDNA, and Facebook Either Individually or Collectively Conducted an Illegal Search of Bebris's Private Facebook Messages.

The Illegal Searches

The information currently available to the defense gives rise to a *prima facie* showing that NCMEC, Facebook and PhotoDNA violated Bebris's Fourth Amendment rights by searching his private Facebook messages without obtaining a warrant. This search and seizure is evident from the discovery and materials provided, but the exact nature and operation of these programs remains somewhat of a mystery, which appears to be by design given the large scale government intrusion into social media sites that are widely used by citizens. This underscores the need to have an evidentiary hearing on this motion.

Furthermore, Bebris is requesting that the Court grant his accompanying Rule 17 motion for subpoenas in order for him to have a fair hearing on whether his rights under the United States Constitution were violated and for this Court to be able to properly consider that question. Without testimony from the proper individuals, there is no way for this Court to truly determine whether the government violated Bebris's Fourth Amendment rights. Thus, Bebris respectfully requests this Court issue a subpoena for the following individuals to testify at an evidentiary hearing:

(1) An employee of Facebook that has knowledge and experience with Facebook's use of PhotoDNA as well as Facebook's policies and procedures regarding the systemic search of users' profiles;

(2) An employee of Microsoft that has knowledge and experience with both the development and use of PhotoDNA; and

(3) An employee of NCMEC that has knowledge and experience with receiving and processing CyberTips as well as NCMEC's policies and procedures regarding such.

Reasonable Expectation of Privacy

"[T]he Fourth Amendment protects people, not places." *Katz*, 389 U.S. at 351, 88 S.Ct. 507. So long as an individual seeks to preserve privacy (even in a public space), the individual has a constitutional right to do so. *Id.* Bebris's subjective expectation of privacy in the private Facebook messages was objectively reasonable. Of the thousands of ways to technologically communicate with another individual, Bebris elected to use the private message feature on Facebook. Like a text message, a private message is shared only with the intended recipients. Thus, Bebris held a subjective expectation of privacy.

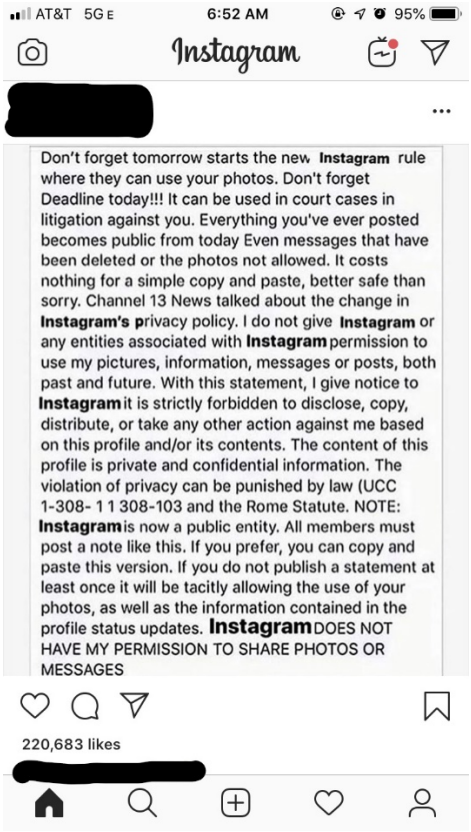
This expectation was objectively reasonable given the state of technology in today's world. "Email has become one of the most common forms of communication, but courts have yet to come to a consensus regarding whether and to what extent a sender has, for Fourth Amendment purposes, a reasonable expectation of privacy in email committed to the custody of an ESP." *U.S. v. Keith*, 980 F.Supp.2d 33, 39 (D. Mass. 2013) (citing *Rehberg v. Paulk*, 611 F.2d 828 (11th Cir. 2010), *aff'd*, 566 U.S. 356, 132 S.Ct. 1497 (2012)). The Sixth Circuit has held that, a person holds a reasonable expectation of privacy in the contents of an email. *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). A Facebook private message has the same characteristics as an email. Further, as

Chief Justice Roberts stated in *Carpenter v. United States*, ___ U.S. ___, 138 S.Ct. 2206, 2217-9 (2018), the "seismic shift in digital technology" precludes a third-party argument that the government can automatically access information stored by a technological third party.

> The vast amount and personal nature of information stored on our electronic devices through websites and apps expands every day and includes not only location information, but our pulse rates, blood pressure, calorie consumption, credit card numbers, prescription and medical information, music and podcast choices, child monitoring cameras, thermostat controls, travel plans and airline tickets, shopping interests and purchases, diary entries and new year resolutions, prayer books, photographs and real time conversations with friends and family members. The list goes on and on and continues to exponentially explode with new technology and applications. Do we automatically relinquish Fourth Amendment protections to this highly personal data because information is no longer physically stored in a file cabinet or bookshelf or a desk drawer, but instead is digitally captured on ah [*sic*] "app" we downloaded on our phone or other internet-connected device from a "third party"?

U.S. v. Wilbert, 2018 WL 6729659, *7 (W.D.N.Y.) (slip copy).

Moreover, as recently as August 20, 2019, a post on Instagram – a company owned by Facebook – regarding privacy on the site went viral. Mike Murphy, *That viral Instagram terms-of-service post is a hoax, so stop reposting it*, MarketWatch (available at https://www.marketwatch.com/story/that-viral-instagram-terms-of-service-post-is-a-hoax-so-stop-reposting-it-2019-08-21); see also Matt Stopera, *A List of All the Celebrities That Fell For That Really Dumb Instagram Hoax*, Buzzfeed (available at https://www.buzzfeed.com/mjs538/heres-a-list-of-all-the-celebrities-that-fell-for-that). The post reads as follows:



The post shows just how much privacy citizens expect or believe they have in their social media communications. Taking society's dependence on technology and social media into consideration, Bebris's expectation of privacy in the private Facebook messages sent over Facebook's messenger application was reasonable.

III. In the Alternative, Law Enforcement Expanded the Scope of the Initial Private Search.

While the Fourth Amendment does not apply to information obtained by a third-party and given to the government, it ***does*** apply if the government "use[s] information with respect to which the expectation of privacy has not already been frustrated." *United States v. Jacobsen*, 466 U.S. 109, 117, 104 S.Ct. 1652 (1984). When the extent of the search by the third party is unknown, case law dictates that courts should err on the side of

caution. See *U.S. v. Keith*, 980 F.Supp.2d 33, 37 (D. Mass. 2013) ("Nothing is known about how the file came to be originally hashed and added to the flat file database, except that it was AOL's practice to hash and add to the database either the hash value of any file that was identified by one of its graphic file analysts as containing child pornography or a hash value similarly generated by a different ESP or ISP and shared with AOL"); see also *Keith* at 42-43.

Here, there is no evidence that shows any employee of Facebook or Microsoft (who developed PhotoDNA) opened or viewed the message containing the alleged child pornography before forwarding it on to NCMEC. Furthermore, there is no evidence that NCMEC opened or viewed the alleged child pornography before passing it on to law enforcement. Therefore, this Court should find that the law enforcement agents expanded the initial private search when the agents opened and examined the photographs associated with the CyberTips.

CONCLUSION

For the above-stated reasons, this Court should grant Bebris's motion to suppress evidence and statements that were fruit of the illegal searches. Additionally, Bebris respectfully requests an evidentiary hearing and leave to file any necessary supplemental briefs following the hearing.

Dated this 22nd day of August, 2019.

Respectfully submitted,

GIMBEL, REILLY, GUERIN & BROWN LLP

By:
/s/ Jason D. Luczak
JASON D. LUCZAK
State Bar No. 1070883
Email: jluczak@grgblaw.com
BRIANNA J. MEYER
State Bar No. 1098293
Email: bmeyer@grgblaw.com
Attorneys for Defendant

POST OFFICE ADDRESS:

Two Plaza East, Suite 1170
330 East Kilbourn Avenue
Milwaukee, Wisconsin 53202
Telephone: 414/271-1440
crim/bebris,alexander/br supp mot to suppress 2019-08-12